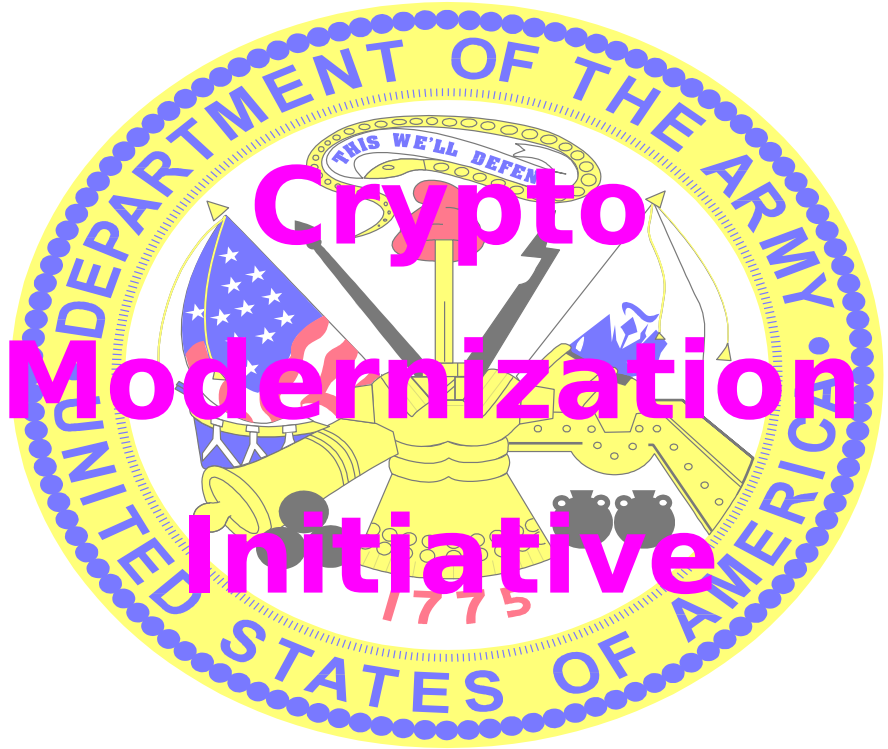


Crypto Modernization Initiative

442nd Signal Battalion
FA 24 Course
US Army Signal Center & Fort Gordon

23 January 2004

Tom Allen **706-791-6767** **(thomas.gerald.allen@us**

Agenda

- Purpose
- Cryptographic Modernization Defined
- Background
- Deficiencies/Crypto Inventory Posture
- Threat
- Directive
- CM Vision/CM Concept
- Core CM Capabilities
- Priority Nine Systems
- Requirements Documentation
- Cost
- Organization Charts
- Wrap-up

Purpose

To Provide an Overview of the Department of Defense Cryptographic Modernization Initiative (CMI) with Focus on the Army CM Program

Cryptographic Modernization (CM) Defined

Cryptographic Modernization (CM) is the Incremental Replacement of DoD's Aging Cryptographic Equipment Inventory to meet Current and Objective Capability Needs. The CM Goal is to Achieve more Robust Security, Network Adaptability (Network-Centric) and Performance Enhanced Equipment Solutions.

Background

FY 99/00 MCEB and NSA Studies Concluded:

- **Crypto Technologically Obsolete 20-30 years old (Losing effectiveness to secure information links)**
- **Cannot Support Network-Centric Architectures**
- **Crypto Inventory Becoming Logistically Unsupportable**

Feb 01 ASD(C3I) Arthur Money memo directs:

- **DoD Working Group Develop Road Map to Address Crypto Systems Upgrade, Replacement or Retirement (NSA, V Grp, Don Heckman, Chair)**
- **Services Procure Modernized Crypto Beginning With FY03-09 POM**

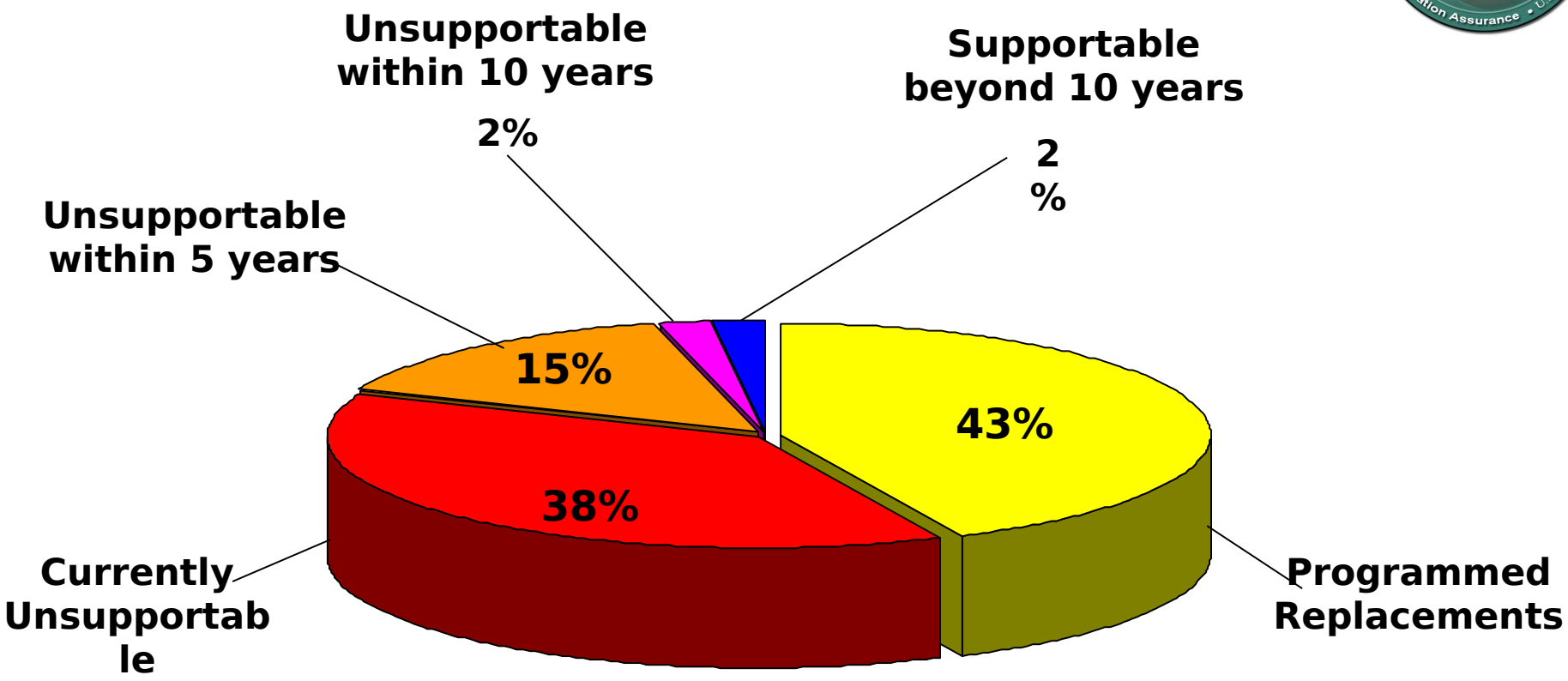
Sep 02 JRB

- **Recognized Nine Crypto Systems as near term Modernization efforts (IFF, KG-30, KI-22, KG-40, CTIC/CDH, KG-94, NES, STU III Replacement, KY-68/78)**
- **Approved Joint Forces Command as CRD Sponsor**
- **Directed Joint Staffing of Crypto Mod MNS and Completion of**

Existing Deficiencies

- **Equipment Obsolescence**
- **Incompatibilities with new architectures and technologies**
- **Non-maintainable equipment**
- **Interoperability and Releasability problems**
  - **Restrictions on key management pose major challenges**
  - **Affects ability to support dynamic communications**
- **Lack of programmability and flexibility**
- **Incompatibility with modernized DoD Key Management Infrastructure**
  - **Lack direct interfaces**
- **Cryptographic equipment shortages**
  - **Readiness and surge capabilities affected**

Inventory Posture



- Current inventory **1.2 Million** Items (Sources: ISSP Database, ATAV, MYNSN, UIT, CMCS)
- Programmed Replacements JTRS, WIN-T, FCS and Other Major Programs.

Threat

- **Continuing trends reflect significantly increased risks of C4ISR, IT, and weapons systems to attacks on cryptography**
  - **Increases in computing power**
  - **Increasing reliance upon Commercial Off-the-Shelf (COTS) systems**
  - **Service/Allied/Coalition use**
  - **Availability of Electronic Warfare Systems**
  - **Widespread distribution of Computer Network Attack (CNA)/Computer Network Exploitation (CNE) tools**

Directive

Memorandum from ASD (C3I), Arthur Money, dated 23 Feb 2001, Subject:

“ The DOD must put into place a cohesive Department-wide initiative which includes the necessary fiscal and implementation planning for upgrade, replacement, and future cryptographic products to ensure our security posture does not continue to erode”….

- Services to POM for Crypto Modernization Initiative Beginning With FY 03-07 POM
- NSA V Group to Chair DoD CMWG with Oversight by ASD(C3I)

CM Vision

Provide High Grade and High Assurance, Scalable, Interoperable, and Network-Centric Cryptographic Solutions that Support Current and Future Forces, Interoperable Across the Joint, Allied, and Coalition Domains.

CM Concept

- **Leverage Latest Technology to Reduce Program Costs and Speed Development Process**
- **Develop Multi-Functional Components that Replace Entire Families of Crypto Equipment (No One-For-One Program Replacements)**
- **NSA Partnership with Services on Program Development**

  NSA will:

  - **Retain Crypto Certification Approval**
  - **Fund Services for Program Development R&D**

  Services will:

  - **Program Funding for Procurement and Fielding**
  - **Conduct Program Development Process**
  - **Develop Equipment Shortage/Supportability Lists**
  - **Prepare Fielding and Transition Plans**

CM Core Capabilities

- Programmable/Reprogrammable Algorithms
- Capable of Receiving an Algorithm Download
- Scalable Components (Software/Component Upgradeable)
- Embedded Modules (Whenever Possible)
- EKMS/KMI Compliant/Capable
- Network-Centric Functionality
- Interoperable with Current Capabilities
- Assured control of DoD networks
- Joint, Allied, Coalition, and Interagency interoperability
- Physical (Form and Fit) Dimensions are Same or Smaller

Priority Nine Systems

PROGRAM	SERVICE LEAD	UTILIZATION
IFF Mode V Craft	Navy	AVN/GND-Air/Water
KG-30 (NC2)	Air Force	Joint Interface
KI-22 (Air Force Only)	Air Force	N/A
KG-40 (LINK 11)	Navy	ADA/Joint Interface
CTIC/CDH	Air Force	Integrated Modules
KG-94 (Family)	NSA	Trunk Encryptors
NES (INE) Encryptors	NSA	Inline Network
STU III Replacement	NSA	Secure Voice/Data
KY-68/78	Army	Tactical DSVT

Requirements Documents

- Mission Needs Statement (MNS) – Approved Mar 03
  - ✓ Request to Use MNS vs. ICD at G3 for Approval
- CRD GO Staffing Complete – JROC (Jan 04)
- Implementation Plan – GO Staffing Complete (Awaiting JROCM)
- Capability Development Document (CDD) Initiated
- Integrated Concept Team (ICT) Initiated
  - ✓ Tier 2 Charter – Approved by CG SIGCEN - Nov 03
  - ✓ ICT First Session Conducted 12-13 Nov at SIGCEN
- STRAP Coordinated W/DOT

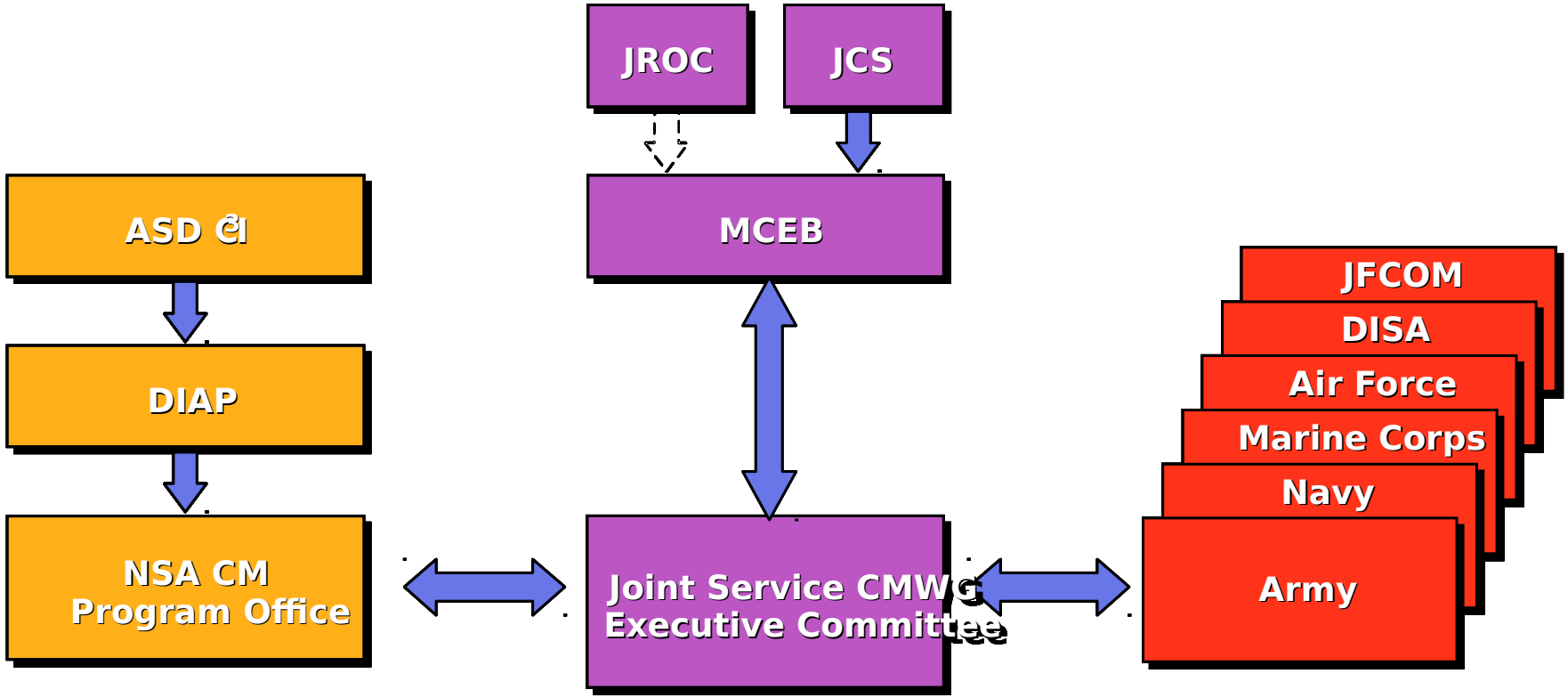
Cost

FY04 DPG Directs Services to Resource CM Effort

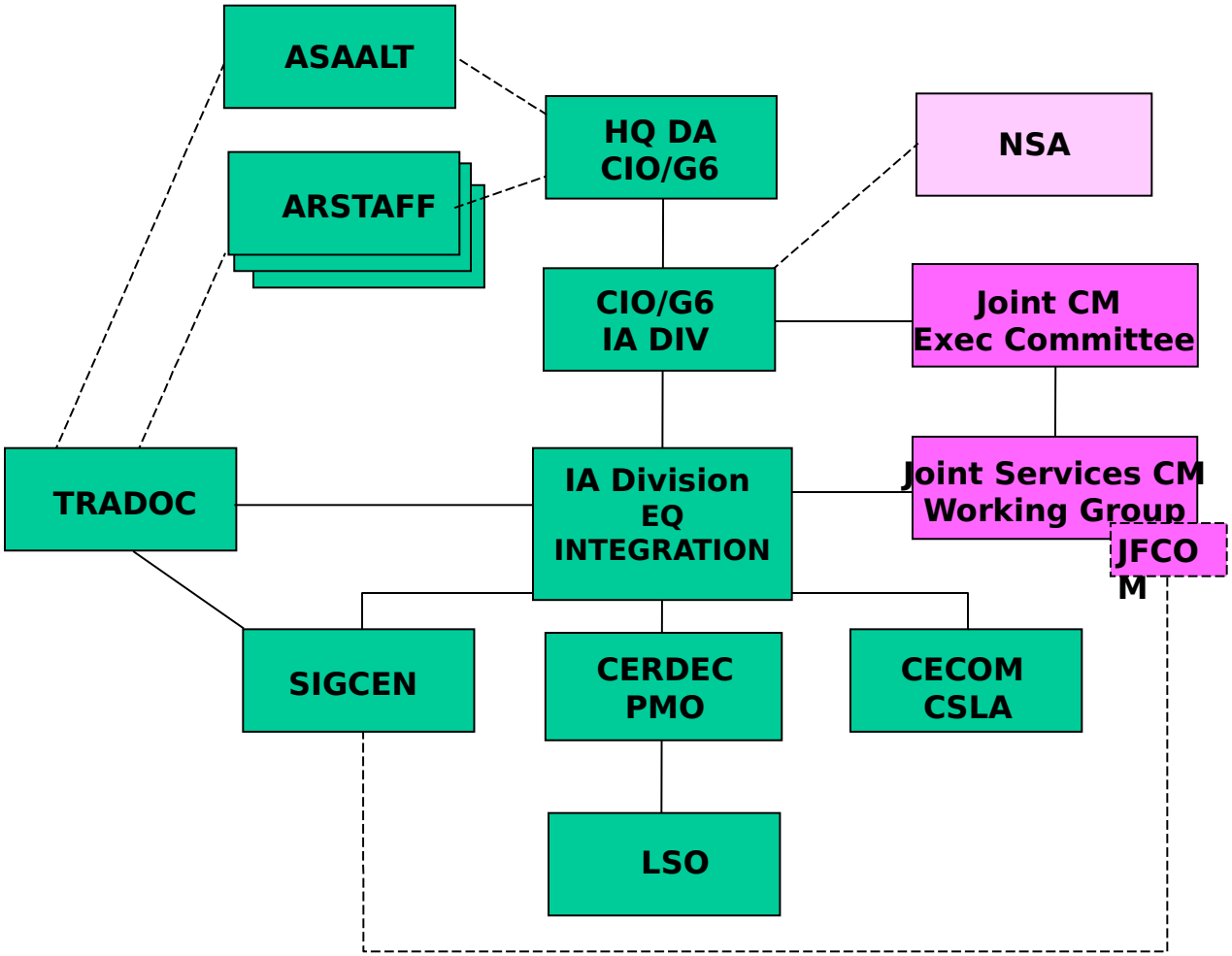
Budget Estimates

- **DoD CM Budget Estimate $6.4B over 4 FYDPs**
- **"Army Only" CM Budget Estimate $1.6B over 4 FYDPs**
- **NSA (DoD) Budget Estimate Only Covers Program**
  - **Research & Development**
- **Services Must Fund All Other Costs**

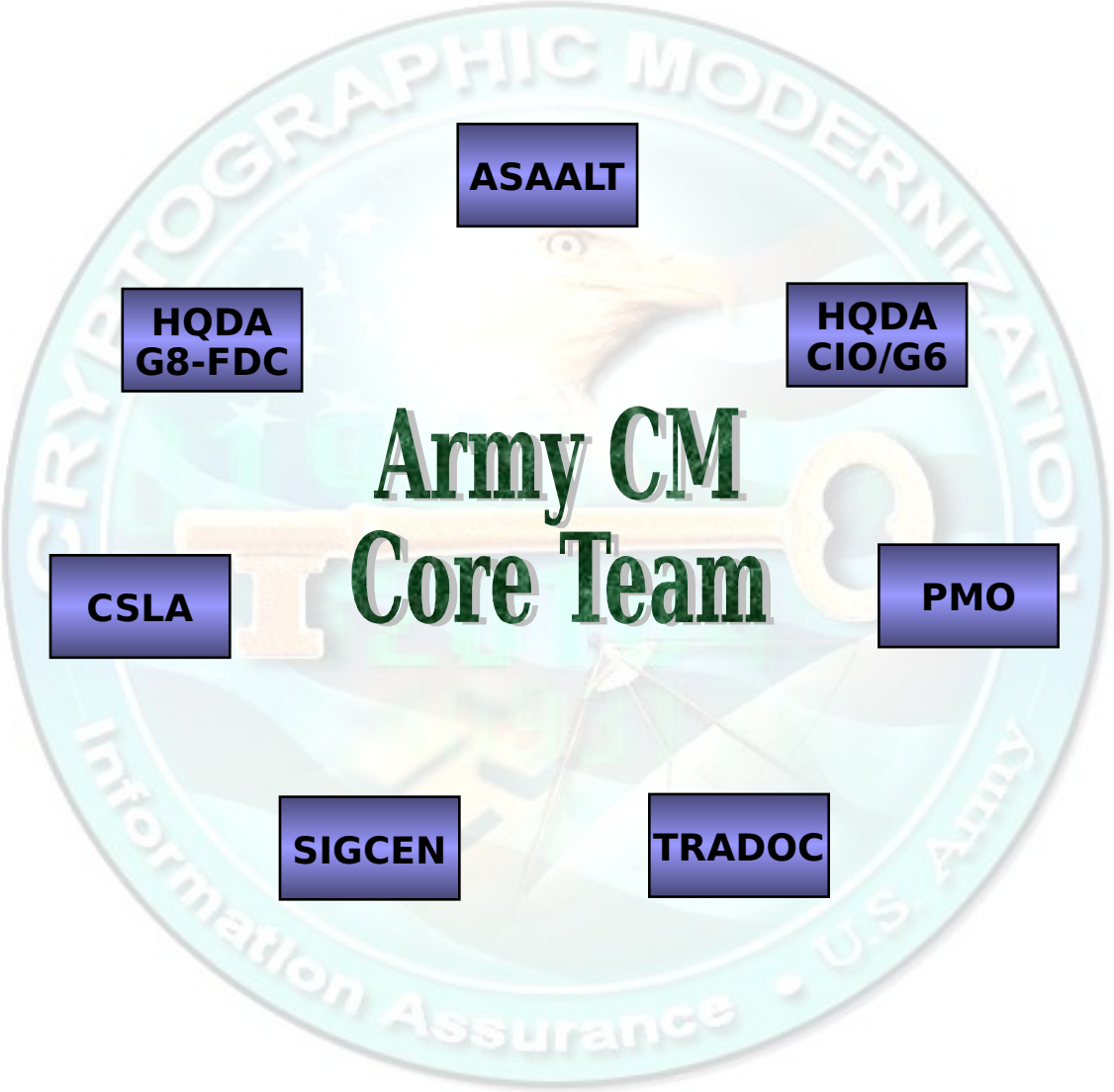
DoD CMI Org Slide



Army Support Staff



CM Management Team



Cryptographic Modernization (Transformation Enabler)

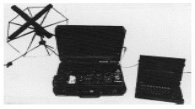
Current Systems
(148 Families)
(>1,200,000 Devices)

CV-3591/
KYV-5

JTIDS
(KGV-8)

Air Data
Terminal

ARC-



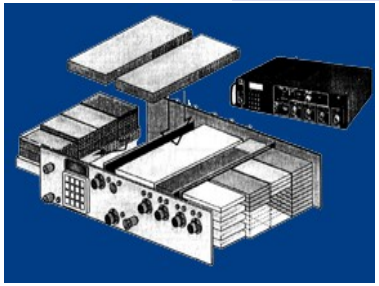
MISTE II
AN/CSZ

PALA (KI-35/36

Modernized Algorithms

Programmability

Flexibility



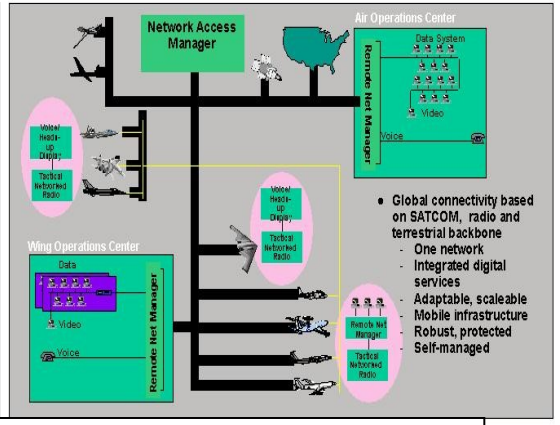
Releasability

Joint / Coalition Interoperability

Key Management Infrastructure

Cross-Cutting Solutions

INTEGRATED DOMAINS



Cryptographic systems provide the underlying information protection foundation that ensures a secure communications environment for

Summary

Cryptographic Modernization is a Crucial C4ISR-IT enabler that is vital to framing Information Superiority as part of the Joint Vision 2020 Operational Capability.

It will implement Multiple, Standardized Algorithm Suites and Operating Modes to Assure Joint Interoperable, Secure C4ISR-IT Systems Communications Among U.S. Allied, Coalition Partner, Military, and Government Entities.

This effort will support the Army's Future Force by leveraging cutting edge technology, speeding up program development and reducing acquisition costs.

QUESTIONS

Contact:

Tom Allen

706-791-6767 or (DSN 780)
(DSN 780)

allent@gordon.army.mil

Dave Houlihan

706-791-2716

houlihad@gordon.army.mil